ABSTRACT OF THE DISCLOSURE

A system and a method to generate cellular automata based random number generators (CA-based RNGs) are presented. A CA-based RNG is where an output of each cell of the CA at time t is dependent on inputs from any cells of the CA (including perhaps itself) at time t – 1. The connections (or inputs) are selected to produce high entropy such that the RNG passes a standard suite of random number of tests, such as the DIEHARD suite. The RNGs may be implemented with field programmable gate arrays.